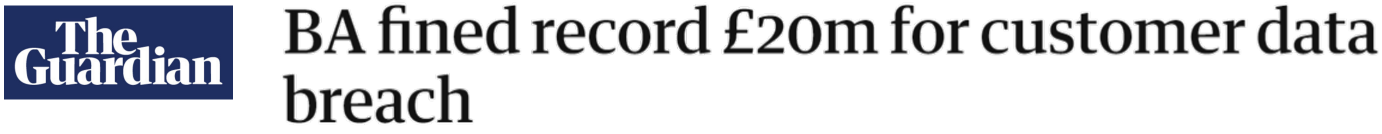
Ready for (nearly) anything: Five things to prepare for a cyber security incident

Gabriel Currie

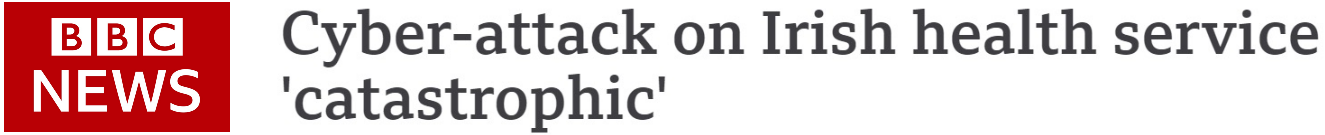
Introduction

- Currently… Cyber Defence Lead @ Cabinet Office
- Previously... Cyber Incident Management @ PwC UK
- Worked on…
  - Building security operations capabilities in government
  - Human-operated ransomware protection and response
  - APT10 “Cloud Hopper” investigation
  - www.ransomwareresponse.org

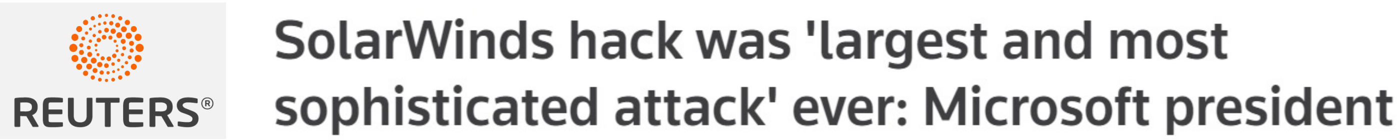
Let’s talk about cyber incidents


The Guardian

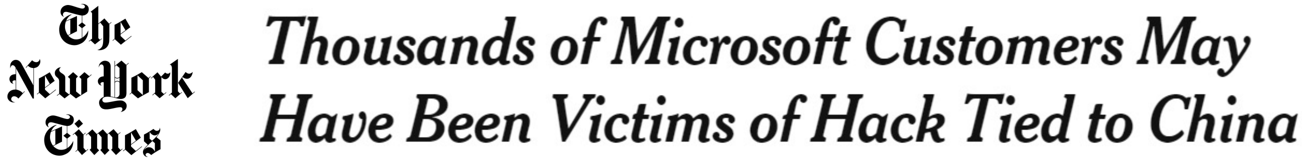
BA fined record £20m for customer data breach



Cyber-attack on Irish health service 'catastrophic'



SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president


The New York Times

Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China

Five things to prepare for a cyber incident

Documented processes with the considerations, decisions and actions to be taken in the event of an incident

Skilled and experienced people to lead, coordinate and execute the response to the incident

Logs to inform the investigation into the incident and help gain an understanding of what has happened, when, and how

Containment and eradication technology to take actions that mitigate risk from the incident

Coordination technology for incident response teams, to communicate and collaborate, delegate and track response actions, and manage delivery

Documented processes with the considerations, decisions and actions to be taken in the event of an incident

Key processes for an incident response team

Incident response plan

- Overarching document detailing what the organisation does during a cyber incident.
- Supported by other high-level documents, e.g., incident management framework, IT incident management plan, disaster recovery plan.

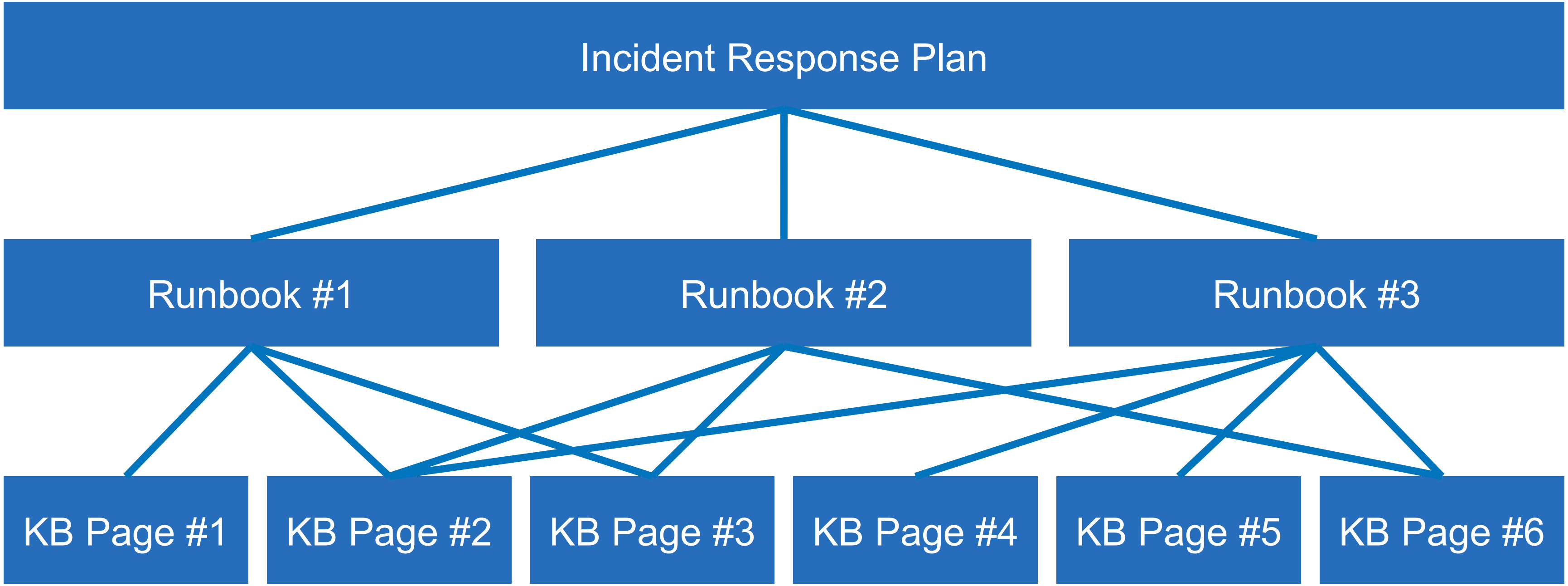
Technical runbooks

- Guidance on what to do in a specific incident scenario.
- Sits underneath (and aligns to) the incident response plan.
- Specific number and nature varies: can be for all scenarios, or just some.

Knowledge articles

- Detailed guidance for completing specific tasks.
- Tasks typically underpin the response to one or more incident scenarios.
- Typically less controlled and more collaborative than other processes.

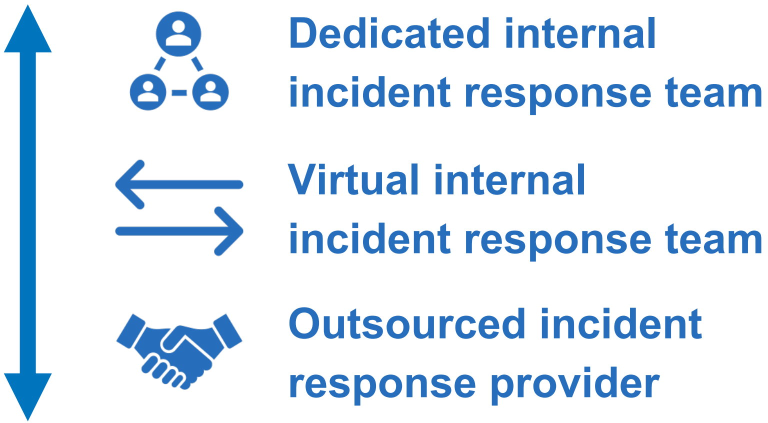
The hierarchy of incident response processes



Skilled and experienced people to lead, coordinate and execute the response to the incident

Resourcing an incident response function

Different models for resourcing:



Dedicated internal incident response team

Virtual internal incident response team

Outsourced incident response provider

If insourcing, you'll want to think about:

- Knowledge, skills and behaviours
- How these map to roles
- Job descriptions
- Framework for learning, development and career progression

Even when outsourcing, you'll still want to think about some of this (and ensure your provider is thinking about the rest).

Roles required for incident response

The **number and nature of roles** should always be driven by the requirements of the organisation and the cyber security team.

Roles can be aligned to existing **frameworks** which define the role itself, and the knowledge, skills and behaviours required across multiple levels:

Skills Framework for the Information Age

NIST Workforce Framework for Cybersecurity

HM Government Security Career Framework

ASD Cyber Skills Framework

Logs to inform the investigation into the incident and help gain an understanding of what has happened, when, and how

What logs to store?

Logging requirements should be driven by:

1. **Real-world threat**: What is the attacker likely to be doing, or trying to do, on my environment?
2. **Investigative requirements**: What will I want to find out about what the attacker has done, or try to confirm that the attacker hasn’t done?
3. **External requirements**: Is there anything that the law, applicable regulations, or internal policy tells us to store or not store?

How long to store logs for?

Logging retention periods should driven by:

1. **Real-world threat (and threat detection capability)**
2. **Investigative requirements**
3. **Infrastructure cost**

Mandiant's 2021 M-Trends report found a median (non-ransomware) dwell-time of **45 days**, with 25% of having a dwell-time of **200+ days**.

If incidents are going to be investigated that occurred 200 days ago, logs should be available to enable this. Balance this against business pressures (i.e. **cost**).

Containment and eradication technology to take actions that mitigate risk from the incident

Host-based containment and eradication

Actions you might want to take include:

- Switching off systems, or restarting systems.
- Isolating hosts from the environment.
- Identifying and removing files from hosts.
- Blocking files from executing on hosts.
- Removing persistence mechanisms from hosts.

Network-based containment and eradication

Actions you might want to take include:

- Blocking known IOCs on external network infrastructure to prevent malware calling home, or the attacker connecting in.
- Isolating one or more areas of the network (especially relevant in a human-operated ransomware attack).

Identity-based containment and eradication

Actions you might want to take include:

- Changing account permissions, access or privileges.
- Resetting individual account credentials (including Active Directory user and service accounts, application accounts, and cloud provider accounts).
- Resetting credentials at scale.
- Disabling accounts.

Coordination technology
for incident response teams to communicate and collaborate, delegate and track response actions, and manage delivery

Coordination technology

How do you ensure you effectively do the following, and is it resilient/secure?

Communicate

Synchronously and asynchronously communicate internally, and with external partners.

Track tasks

Document tasks required to respond to the incident, tracking due dates, effort, status, assignees, next steps.

Collaborate

Collaborate on analysis, response and documentation tasks.

Report

Capture key statistics for each incident and output these to enable management reporting.

Five things to prepare for a cyber incident

Documented processes with the considerations, decisions and actions to be taken in the event of an incident

Skilled and experienced people to lead, coordinate and execute the response to the incident

Logs to inform the investigation into the incident and help gain an understanding of what has happened, when, and how

Containment and eradication technology to take actions that mitigate risk from the incident

Coordination technology for incident response teams, to communicate and collaborate, delegate and track response actions, and manage delivery

Any questions?